

IN THE UNITED STATES DISTRICT COURT
FOR THE EASTERN DISTRICT OF VIRGINIA
ALEXANDRIA DIVISION

IN RE: CAPITAL ONE CONSUMER DATA
SECURITY BREACH LITIGATION

MDL No. 1:19md2915 (AJT/JFA)

This Document Relates to the Consumer Cases

**MEMORANDUM IN SUPPORT OF PLAINTIFFS' MOTION TO COMPEL
DISCOVERY FROM THE AMAZON DEFENDANTS**

Plaintiffs submit this Memorandum in Support of their Motion to Compel Discovery from the Amazon Defendants ("AWS") regarding three requests for production of documents and one related Rule 30(b)(6) topic – all of which Plaintiffs believe are relevant and proportional to the needs of the litigation.¹

First, Plaintiffs seek documents and communications "relating to other AWS customers that Paige Thompson targeted, attacked or breached, in which AWS services (including the EC2 Instance Metadata Service, Identity and Access Management roles, security credentials, S3 storage, or GuardDuty) were implicated, exploited or avoided." *See* Ex. A, AWS's Objections to Plaintiffs' Third Requests for Production of Documents, at Request 57. This request was served on October 21, 2020 after AWS witnesses testified that 71 other AWS customers had been targeted by Paige Thompson – the attacker who perpetrated the Data Breach against Capital One – and that AWS had notified those customers and conducted an investigation into Thompson's attacks.

¹ Plaintiffs conferred telephonically on November 9 and 12 about the three document requests, and Amazon stated that it was standing on its objections. Plaintiffs, while reserving their rights, did proffer a proposed compromise, which Amazon stated it would respond to by Friday, November 13 or Monday, November 16. However, those dates came and went without any response. When Amazon finally did respond on November 19, stating it would accept the compromise, it imposed limitations that were unacceptable to Plaintiffs; therefore, Plaintiffs informed Amazon that they intended to move to compel, and the parties agreed the issue required Court intervention.

However, none of the witnesses questioned by Plaintiffs, even those involved in the investigation, could recall any specifics about the customers or what AWS found in its investigation. After receiving the request, AWS objected to providing the requested documents on November 5, 2020 and informed Plaintiffs on a November 9, 2020, meet and confer regarding the request that it would be standing on its objections even though its responses have not yet been served. Accordingly, Plaintiffs move to compel production of these highly relevant documents.

Second, Plaintiffs seek documents relating to AWS's relationship and provision of services to Capital One, which specifically target an understanding of the services provided and the financials related to those services. Ex. F, Amazon's Responses and Objections to Plaintiffs' Second Requests for Production at Request Nos. 50 and 52. These targeted requests are relevant to Plaintiffs' development of evidence for their damages claims against AWS, which the Court has recognized. *See, e.g.*, Dkt. 879 at 45 (explaining that the profits AWS received by charging Capital One for server use, storage, and retention of the data involved in the Data Breach without "securing the data would be 'unjust'"). Moreover, Plaintiffs noticed a related Rule 30(b)(6) topic, which AWS first objected to on the eve of the deposition stating it would not provide a witness. Ex. G, Objections to Rule 30(b)(6) Notice. To the extent the Court grants Plaintiffs' Motion with respect to Request 50, Plaintiffs also respectfully request that the Court compel AWS to produce a witness on the related topic.

LEGAL STANDARD

"Parties are entitled to discover any material that is relevant to any party's claim or defense, is nonprivileged, and proportional to the needs of the case." *BASF Plant Sci., LP v. Commonwealth Sci. and Indus. Research Org.*, No. 2:17-cv-503, 2019 WL 8108060 (E.D. Va. July 3, 2019) (Morgan, J.) (citing Fed. R. Civ. P. 26(b)(1)). Relevance in this context is to be read liberally. *Id.*;

Fed. R. Civ. P. 26(b)(1) (“Information within this scope of discovery need not be admissible in evidence to be discoverable). Proportionality considers: “the importance of the issues at stake in the action, the amount in controversy, the parties’ relative access to relevant information, the parties’ resources, the importance of the discovery in resolving the issues, and whether the burden or expense of the proposed discovery outweighs its likely benefit. *Id.* Accordingly, “[t]he Federal Rules contemplate the broadest discovery possible in the search for the truth.” *Id.* (quoting *Doe v. Old Dominion Univ.*, 289 F. Supp. 3d 744, 749 (E.D. Va. 2018) (Morgan, J.)); see *Seldowitz v. Office of Inspector Gen. U.S. Dept. of State*, 238 F.3d 414 (Table), 2000 WL 1742098, at *5 (4th Cir. Nov. 13, 2000); *Minor v. Bostwick Lab’s, Inc.*, No. 3:09-cv-343, 2012 WL 13028138 (E.D. Va. July 13, 2012) (Novak, J.).

“Pursuant to Federal Rule of Civil Procedure 37(a), a party may move for an order compelling disclosure or discovery. Fed. R. Civ. P. 37. Local Rule 37(A) further provides: ‘After a discovery request is objected to, or not complied with, within time, and if not otherwise resolved, it is the responsibility of the party initiating discovery to place the matter before the court by a proper motion...to compel an answer, production, designation, or inspection.’” *Addax Energy SA v. M/V Yasa H. Mulla*, No. 2:17-cv-641, 2018 WL 10470917, at *3 (E.D. Va. Nov. 13, 2018) (Morgan, J.) (marks in original). The Court is afforded broad discretion in this regard. *Rowland v. Am. Gen. Fin., Inc.*, 340 F.3d 187, 195 (4th Cir. 2003); *Lone Star Steakhouse & Saloon, Inc. v. Alpha of Va.*, 43 F.3d 416, 426 (4th Cir. 1996); *Wu v. Tseng*, No. 2:06-cv-346, 2007 WL 4143077, at *3 (E.D. Va. Nov. 19, 2007) (Morgan, J.).

“[T]he party or person resisting discovery, not the party moving to compel discovery, bears the burden of persuasion.” *Addax Energy*, 2018 WL 10470917, at *4 (quoting *Eramo v. Rolling Stone, LLC*, 314 F.R.D. 205, 209 (W.D. Va. 2016) (Conrad, J.) (marks in original); *Old Dominion*,

289 F. Supp. 3d at 749. Particularly when electronically stored information (“ESI”) is implicated, “the party resisting its production must show that the ESI is not reasonably accessible due to burden or cost, and, even if such a showing is made, the Court may nevertheless order its production if the requesting party shows good cause, keeping in mind Rule 26(a)(2)(C).” *Id.*

ARGUMENT

A. Documents Relating to Paige Thompson’s Hacks or Attempted Hacks of 71 Other AWS Customers

This case involves a Data Breach perpetrated by a former AWS employee, Paige Thompson, against Capital One, who was storing the personal information of nearly 100 million Americans on the AWS cloud product. Discovery has revealed that in targeting Capital One, Thompson also targeted other AWS customers through similar attacks.

AWS’s Rule 30(b)(6) witness, Stephen Schuster (Director of Security Engineering and Operations), testified that Thompson targeted 71 other AWS customers. *See* Ex. B, Rule 30(b)(6) (Schuster) Dep. Tr. 157:19-22. He further testified that AWS only learned of the 71 other customers after learning of Capital One’s Data Breach, and that, thereafter, AWS notified those other customers:

Q. Upon learning through a text on July 20th of the data breach, did Amazon notify its other customers utilizing its cloud systems of the breach?

A. We were provided indications that Paige had accessed -- potentially accessed other customers using this method. And so yes, we did provide that notification.

...

Q. And how many customers in total were in that universe?

A. The first set was 11, and then I believe we had another set that we heard through the law enforcement investigations and, in that, there was around 60.

Q. So in addition to Capital One, Ms. Thompson was able to get into the accounts of 71 additional customers of AWS?

A. I do not know the success or the failure of her ability to get into those other customers. We had information that they were a focus of her time. I do not have the information of whether she was successful or not or whether other data were actually exfiltrated or accessed.

Id. at 156:19-25, 157:17-158:6. He testified that the 71 customers were notified because “Paige Thompson might have engaged in some malfeasance in connection with their accounts” and that AWS had information that “Paige Thompson was paying attention to [their] environments”; therefore, AWS told the customers that they “should look deeply at what’s going on” and “should know how and what happened with Capital One.” *Id.* at 163:6-164:3.

Yet, Mr. Schuster was unable to provide any specifics with respect to the nature of the attacks – for example, whether they were similar to the Capital One Data Breach (*id.* at 157:1-16) – or whether the customers were similar to Capital One:

Q. Were any of the 71 financial institutions?

A. I don’t know. I don’t know who those customers were.

Q. Were any of the 71 customers, however, regardless of whether or not you know or don’t know their identities, store information of customers or consumers?

A. I -- I -- I don’t know what was -- much like with Capital One, I don’t have the ability to know how their environment is set up, if the attacks were successful, or where any or even what data is stored in their environments.

Q. What period of time did the attacks on these 71 accounts occur?

A. I do not know[.]

Id. at 159:2-16. The witness testified that he was not the one who performed the “analysis” on these customers. *Id.* at 159:25-160:3.

Plaintiffs thereafter attempted to elicit more specific testimony on this topic in order to determine whether those other attacks were similar to the one perpetrated by Thompson on Capital One’s AWS cloud. Plaintiffs pursued this inquiry because if Thompson exploited similar

vulnerabilities in 71 *other* AWS customer clouds, that fact is highly pertinent to the question of whether the AWS cloud contains pervasive vulnerabilities that caused or contributed to the Data Breach at issue in this case, or as Amazon has claimed, all the blame for the Breach should lie with Capital One. Despite Plaintiffs' attempts, AWS witnesses, like Mr. Schuster, could recall little by way of specifics.

For example, Stephen Schmidt, AWS's Chief Information Security Officer, testified that AWS had conducted an investigation into Thompson's activity with respect to other customers, but could not recall the results of that investigation. He further testified that the investigation was led by Mr. Schuster who, as shown *supra*, could also not recall specifics and who testified he was not involved in the investigation.

Q. Is it your understanding that -- or were you told that Paige Thompson had claimed to have done the same thing to other customers, Ford, Ohio State University and others?

A. Michael Johnson had repeated to me that Paige claims to have done the same thing to other customers.

Q. And after having been told that by Mr. Johnson, did you undertake any investigation or have anyone in your command undertake any investigation to determine whether or not that had, in fact, occurred?

A. Yes.

Q. And what was discovered?

A. I don't know the results of that. I don't recall.

Q. Who did you instruct or communicate to undertake that investigation?

A. It would have been my security operations team.

Q. And who was the team that led that in July --

A. Steven Schuster.

See Ex. C, Schmidt Dep. Tr. 113:12-114:8.

Then in early October, Justin Christian (Senior Data Scientist) testified he was involved in the investigation of the other AWS customers targeted by Thompson but testified that he recalled no specifics of the investigation or any conclusions:

Q. Were you also involved in some investigations regarding whether other companies were compromised by Paige Thompson -- other AWS customers were compromised by Paige Thompson?

A. Yes, although to what extent I can't recall.

Q. Did you come to any conclusions about whether other customers had been compromised by her?

MR. NEWBY: Objection.

A. I don't -- I don't recall coming to any such conclusions.

BY MR. BARTHLE: Q. Were you just unable to reach a conclusion or you just don't remember what they were?

A. I do not recall if a conclusion was actually reached.

Q. Do you recall which customers you investigated on that issue?

A. I do not specifically recall which customers I investigated.

Ex. D, Christian Dep. Tr. 130:14-131:19.

On October 21, similar testimony was elicited from Vince Passaro (Manager of Security Engineers) who was involved in AWS's inquiry into the other customers according to an email produced in the litigation, but could recall next to nothing by way of specifics. *See* Ex. E, Passaro Dep. Tr. 60:3-5 (when asked whether "it was ever determined by Amazon that Paige Thompson compromised other Amazon customers," responded: "I don't know"); *id.* at 65:16-23, 68:18-22 (testifying that he "did not recall" an email chain he received regarding the FBI victim list sent to Amazon, and that he did not "recall the outcome [of the analysis discussed in the chain], no").

Because Plaintiffs were unable to elicit specific testimony from the witnesses, the same day as Mr. Passaro's deposition on October 21, 2020 (during which he could recall no specifics),

Plaintiffs served their Third Requests for Production on AWS seeking the documents that would elucidate the information Plaintiffs sought. Request 57 seeks documents and communications “relating to other AWS customers that Paige Thompson targeted, attacked or breached, in which AWS services (including the EC2 Instance Metadata Service, Identity and Access Management roles, security credentials, S3 storage, or GuardDuty) were implicated, exploited or avoided.” *See* Ex. A. Essentially, Plaintiffs seek documents relating to the *same* hacker’s *similar* exploitation of AWS cloud products around the *same* time-period as the Capital One Data Breach. These documents include the notices sent to customers and documents detailing what AWS learned from those customers and its own investigation about the nature of Thompson’s targeting of those customers. Given AWS seemingly did not even issue a formal report with respect to the Capital One Data Breach, Plaintiffs have also requested communications related to this topic, as AWS appears to assess and report on security issues affecting its customers – even large ones – via email and more unofficial correspondence channels.

AWS objected to this request, stating that it believed the request was unduly burdensome and disproportionate to the needs of the litigation. However, AWS did not articulate to Plaintiffs the specific cost of the burden it asserted, nor did it articulate any specific reasons as to why it believed the information irrelevant. This is likely because AWS knows the information is relevant to the claims against it and producing it will impose no undue burden. AWS is a large corporation who had a former employee target 72 of its customers’ AWS clouds. One of those targets was Capital One, and as a result, approximately 98 million Americans’ information is now compromised. Amazon has taken the position any blame must be Capital One’s, but that defense would fall if dozens of other customers were also compromised through the same AWS cloud vulnerability. Plaintiffs attempted to assess the similarity of the other attacks by eliciting testimony

from those who should know, including AWS's CISO, but were rebuffed by the witnesses' lack of recollection. Therefore, the only way to gain access to this highly relevant information is through the documentary evidence, which AWS does not deny exists. For these reasons, the Court should order production of the requested documents.

B. Documents and Deposition Testimony Relating to the Services Provided by AWS to Capital One

Plaintiffs have also requested targeted documents that seek to develop needed evidence of the damages Plaintiffs are entitled to in this case. Plaintiffs served these requests on October 8, Amazon objected on November 5, the Parties discussed on November 9 and 12, and AWS served its responses on November 16.

First, Request 50 seeks: "All agendas, minutes, presentations, and notes concerning meetings of Your Board of Directors, or any committee of Your Board of Directors, at which the relationship with Capital One was discussed, including discussion of any and all negotiations for any services to be provided to Capital One, and the revenue and profit, potential as well as what was eventually realized by You, from such services." AWS stated it would not produce documents responsive to this request. Ex. F at Request No. 50. This is a targeted request, which seeks financial information regarding the services AWS provided to Capital One – such as storage, computing, and security products, all of which are relevant to Plaintiffs' damages discovery (*see, e.g.*, Dkt. 879 at 45) – as presented by management to the Board. Plaintiffs have thus far received general information on the revenues received from specific services by AWS from Capital One to date. Therefore, the presentations by management to the Board regarding Capital One's account and Board materials relating to the Capital One relationship are a likely repository of this relevant information. Such a search and production of this obviously relevant material requires little to no

burden. AWS can simply run a search over its Board materials for discussion of Capital One, review those likely limited number of documents, and produce them to Plaintiffs.

Relatedly, should this Court grant Plaintiffs' Motion with respect to Request 50, Plaintiffs request the Court also compel AWS to provide a corporate representative to testify as to Plaintiffs' Second Rule 30(b)(6) Topic 3: "Facts and circumstances regarding meetings at which Your Board of Directors, or any committee of Your Board of Directors, discussed the relationship with Capital One, including discussion of any and all negotiations for any services to be provided to Capital One, and the revenue and profit, potential as well as what was eventually realized by You, from such services." Plaintiffs noticed this topic on October 13. AWS first raised objections to this topic on November 16 the *night before* the deposition was to take place on November 17. That night, AWS informed Plaintiffs for the *first time* that it would not be producing a corporate representative as to three of the seven topics. *See* Ex. G, Objections to Rule 30(b)(6) Notice; Ex. H. Nov. 16, 2020 Emails between T. Newby and B. Vahle. Not only should AWS have informed Plaintiffs in advance that it would not be producing a deponent, but it should have moved for a Protective Order. *See Beach Mart, Inc. v. L&L Wings, Inc.*, 302 F.R.D. 396, 406 (E.D.N.C. 2014) ("The proper procedure to object to a Rule 30(b)(6) deposition notice is not to serve objections on the opposing party, but to move for a protective order.").

Second, Request 52 seeks: "Documents sufficient to show the services offered and made available by You to Capital One, including Proposals, estimated savings by utilizing Your services, any comparisons of Your services and fees to any of Your competitors, and any savings that Capital One would realize by choosing You over maintaining consumer data on its own servers." AWS objected to producing documents responsive to this request and informed Plaintiffs it was standing on its objections. Ex. F at Request No. 50. However, these documents are certainly

relevant. AWS has produced perfunctory information about the services it provides Capital One and the revenue derived therefrom. Plaintiffs can present a damages analysis based on this information, but will need to better understand the exact services provided by AWS to Capital One under the contract, the nature of those services, and the financial information associated with those services to respond to anticipated attacks on Plaintiffs' presentation to the jury.

For example, the data at issue in this Data Breach was stored on the AWS cloud; therefore, information about the costs, savings, and revenues associated with storage are certainly relevant. But also relevant are the costs, savings, and revenues associated with computing because the AWS cloud is not simply a storage unit: the computing services provided by AWS work hand-in-hand with the storage of the data, which cannot be stored, retrieved, or accessed without the computing power. Similarly, services such as Amazon Macie, as just one example – which Capital One was using to identify where it had stored customer information so that it could presumably better protect it – are likewise relevant. Thus far, Plaintiffs have only been provided with bare-bones numbers associated with names of services showing the revenues of each with respect to Capital One. However, Plaintiffs are entitled to more fulsome information to assess not only the services and how the services interrelate, but also the contours of the financial relationship between Capital One and Amazon. Indeed, as the Court held in its Order on the Motions to Dismiss, Amazon's retention of profits it received from Capital One's use of the AWS cloud to store and utilize the data involved in the Data Breach without "securing the data would be 'unjust.'" Dkt. 879 at 45. And, Amazon has articulated no specific burden to producing these materials to Plaintiffs and can articulate no such burden. Plaintiffs request – which requests only documents "sufficient to show" – is proportional to the needs of the litigation.

CONCLUSION

For all the reasons set forth above, Plaintiffs have satisfied their requirement of a prima facie showing that the documents relating to hacker Paige Thompson's intrusions on 71 other AWS customers and documents and deposition testimony relating to AWS's provision of services to Capital One are relevant and proportionate to the needs of this case. Plaintiffs respectfully request that the Court issue an order compelling AWS to produce the requested documents and related deposition testimony, and any other relief this Court deems proper.

Dated: November 20, 2020.

Respectfully Submitted,

/s/ Steven T. Webster
Steven T. Webster (VSB No. 31975)
WEBSTER BOOK LLP
300 N. Washington Street, Suite 404
Alexandria, Virginia 22314
Tel: (888) 987-9991
swebster@websterbook.com

Plaintiffs' Local Counsel

Norman E. Siegel
STUEVE SIEGEL HANSON LLP
460 Nichols Road, Suite 200
Kansas City, MO 64112
Tel: (816) 714-7100
siegel@stuevesiegel.com

Karen Hanson Riebel
**LOCKRIDGE GRINDAL NAUEN,
P.L.L.P**
100 Washington Avenue South, Suite 200
Minneapolis, MN 55401
Tel: (612) 339-6900
khriebel@locklaw.com

John A. Yanchunis
**MORGAN & MORGAN COMPLEX
LITIGATION GROUP**
201 N. Franklin Street, 7th Floor
Tampa, FL 33602
Tel: (813) 223-5505
jyanchunis@ForThePeople.com

Plaintiffs' Co-Lead Counsel

CERTIFICATE OF SERVICE

I hereby certify that on November 20, 2020, I electronically filed the foregoing document with the Clerk of the Court using the CM/ECF system, which will send notice of electronic filing to all counsel of record.

/s/ Steven T. Webster
Steven T. Webster (VSB No. 31975)
WEBSTER BOOK LLP